On Spatial Security Outage Probability Derivation of Exposure Region Based Beamforming with Randomly Located Eavesdroppers

Yuanrui Zhang*, Youngwook Ko*, Roger Woods*, Alan Marshall§, Joe Cavallaro‡, Kaipeng Li‡,
* ECIT, Queen's University Belfast
Belfast, Northern Ireland, UK
Email: {yzhang31,y.ko,r.woods}@qub.ac.uk
§ Electrical Engineering and Electronics, University of Liverpool
Liverpool, England, UK
Email: Alan.Marshall@liverpool.ac.uk
† Department of Electrical and Computer Engineering, Houston, Texas, USA
Email: {cavallar, kaipeng.li}@rice.edu

***Abstract*—This paper presents the closed-form expression for a circular array, of the spatial security outage probability which is a novel performance metric that measures the security level of the legitimate transmission from the spatial aspect in the presence of Poisson Point Process distributed eavesdroppers. In this paper, it is shown how beamforming is used to create an exposure region where any randomly located eavesdropper causes secrecy outage, based on which the general expression of the spatial security outage probability is derived. Using this, the closed-form expression is obtained for the circular array, which reveals the impact of the array parameters on the security performance.**

I. Introduction

With the ubiquitous utility of wireless communications, the need to develop higher level security has grown stronger. Physical layer security has recently received much attention as a complementary approach to the traditional encryption techniques in the higher layers [1]. Much research has been based on Wyner's wiretap channel model [2] and has been extended to various channel models (see [3] and references therein). However, the large-scale path loss has not been considered to any great extent as users are often randomly distributed, and it has only been with recent developments in stochastic geometry theory, e.g., via Poisson point process (PPP) [4], [5], that the distribution of the random users' locations can be modeled.

Users' locations provide an intrinsic distinction for the related channels because the large-scale path loss is related to users' distances to the transmitter. In Wyner's wiretap channel model, the legitimate user should have a better channel than the eavesdropper. Therefore, the user's location should be taken into account when considering a secure transmission for the legitimate user in presence of eavesdroppers. In this paper, we consider the classic model of Alice, Bob and Eve(s) and the scenarios that only Bob's location information is available at Alice, as explained in [6]. Alice is equipped with uniform circular array (UCA) and wishes to transmit to Bob in presence of PPP distributed Eves. Bob and Eves are assumed to have a single antenna, and beamforming based on Bob's location information is performed to create the exposure region (ER) where any Eve inside causes secrecy outage to the legitimate transmission.

There has been work that considers the physical region related to secure transmissions [5]–[9]. However, in [7], the physical region is not based on the information-theoretic parameters, thus is not subject to formal analysis. In [5], [6], [8], [9], the physical region is based on the secrecy outage probability, but array parameters are overlooked. Since beamforming is performed via antenna arrays, the ER created by using beamforming is highly related to the array parameters and can be controlled by changing the array parameters.

In this paper, the ER-based beamforming is introduced for the first time to introduce physical layer security from the spatial aspect. To this end, a novel performance metric, i.e., the spatial secrecy outage probability (SSOP), is derived to measure the security level of the legitimate transmission. This allows analysis of the impact of the array parameters on the security performance. To begin with, a free-space channel model is used as a guidance for fading channels as well. The SSOP can be applied to conduct information-theoretic analysis for previous work [7] and can extend the work in [5], [8], [9] by analyzing the security performance with respect to the array parameters. The main contributions of the paper are:

- Establishment of the concept of the ER based on the secrecy outage probability and development of the SSOP to measure the physical layer security level for the free-space channel for the first time;
- Derivation of the closed-form relationship between the SSOP and UCA parameters, i.e., number of elements and radius;
- Analysis of the impact of the array parameters.

The paper is organized as follows. In Section II, the system and channel models are introduced. In Section III-A, the ER and the SSOP for a general array are introduced and followed by the derivation of the closed-form expression of the SSOP for a UCA. In Section IV, the impact of the array parameters is analyzed and followed by the conclusions in Section V.

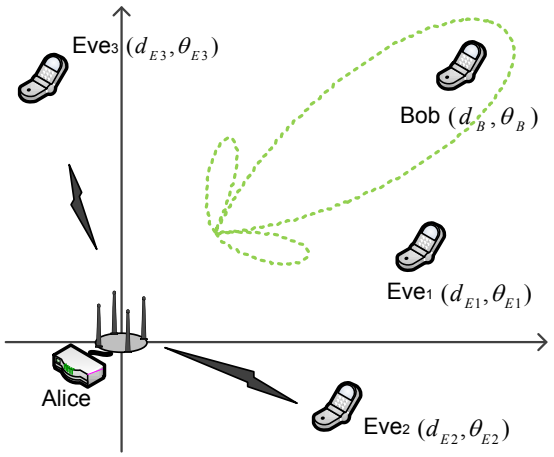

Fig. 1. An example of a wireless security communications system with one AP, i.e., Alice, Bob and homogeneous PPP distributed Eves

II. System and Channel Models

Consider secure communications in a wireless local access network, where the access point (AP), Alice, communicates to a desired receiver (Bob) in presence of passive eavesdroppers (Eves), as shown in Fig. 1. Let's suppose that the AP is equipped with a UCA having N antenna elements with radius R, where λ is the wavelength of the carrier signal [10]. Bob and Eves are assumed to have a single antenna and are simply referred to as a 'general user' or a 'user' hereinafter, unless otherwise stated.

We consider that the AP is located at the origin point, as shown in Fig. 1. Assume that the users are distributed by a homogeneous PPP, Φ_e, with density λ_e [4]; the user's coordinates are denoted by $z = (d, \theta)$. Thus, Bob's coordinates are denoted by $z_B = (d_B, \theta_B)$; the i^{th} Eve's coordinate is $z_{Ei} = (d_{Ei}, \theta_{Ei}), \forall i \in \mathbb{N}^+$. The subscripts '$_B$' and '$_E$' are used for Bob and Eves hereinafter.

Given z_B, the AP transmits data only towards Bob in the presence of l randomly distributed Eves in every transmit time interval. In particular, let x be the modulated symbol with unit power, $\mathbb{E}[|x|^2] = 1$, and P_t be its transmit power. The transmitted vector, denoted by $\mathbf{u}$, is given by $\mathbf{u} = \sqrt{P_t}\mathbf{w}^* x$, where $\mathbf{w}$ is the beamforming weight vector, i.e., $\mathbf{w} = \mathbf{s}(\theta)/\sqrt{N}$, and $\mathbf{s}(\theta)$ is the array steering vector for the UCA,

$$\mathbf{s}(\theta) = [1, ..., e^{-jkR\cos(\theta-\psi_i)}, ..., e^{-jkR\cos(\theta-\psi_N)}]^T, \quad (1)$$

where $\theta \in [0, 2\pi]$, $\psi_i = 2\pi(i-1)/N$ and $k = 2\pi/\lambda$, and λ is the wavelength of the carrier signal, which for the 2.4 GHz Wi-Fi signal is 12.5 cm. When θ is set to θ_B, i.e., $\mathbf{w} = \mathbf{s}(\theta_B)/\sqrt{N}$, the received power at Bob is maximized.

For a general user at $z = (d, \theta)$, denoted by $\mathbf{h}(z)$, the channel gain vector between the AP and user at z can be expressed by

$$\mathbf{h}(z) = d^{-1}\mathbf{s}(\theta), \quad (2)$$

where d^{-1} denotes the free-space path loss at the distance d. According to (2), the received signal at z can be obtained by

$$r(z) = \mathbf{h}^T(z)\mathbf{u} + n_W = \frac{\sqrt{P_t}}{d} G(\theta, \theta_B)x + n_W, \quad (3)$$

where n_W is the additive white Gaussian noise with zero mean and variance σ_n^2 and $G(\theta, \theta_B)$ is the array factor and is given by

$$G(\theta, \theta_B) = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} e^{jkR[\cos(\theta_B-\psi_i)-\cos(\theta-\psi_i)]}. \quad (4)$$

Denoted by $\gamma(z)$, the received SNR at z, can be found from (3),

$$\gamma(z) = \frac{P_t G^2(\theta, \theta_B)}{\sigma_n^2 d^2}. \quad (5)$$

The channel capacity of the general user at z can be given by

$$C(z) = \log_2[1 + \gamma(z)] = \log_2\left[1 + \frac{P_t G^2(\theta, \theta_B)}{\sigma_n^2 d^2}\right]. \quad (6)$$

For convenience, let $C_B = C(z_B)$ and $C_{Ei} = C(z_{Ei})$ denote the channel capacities of Bob and the i-th Eve hereinafter. A proper design of $G(\theta, \theta_B)$ can improve C_B while decreasing C_{Ei}.

III. Exposure Region and Spatial Secrecy Outage Probability

From (6), it can be noticed that C_{Ei} relies on a random location z_{Ei}. As a result, one or more Eves could have a higher channel capacity than a certain threshold, leading to the secrecy outage [11]. For given Eves' random locations, the exposure region (ER) is mathematically formulated to characterize the above secrecy outage event. Then the SSOP with respect to the ER is evaluated as a measure of the security level.

A. Exposure Region

Let R_B and R_s be the rate of the transmitted codewords and the rate of the confidential information, respectively, As in [11], we differentiate a secrecy outage and a unreliable transmission, i.e., a data outage when $C_B < R_B$. In this paper, we only focus on a secrecy outage event, given that $C_B \geq R_B$. Notice that the data outage event, given that $C_B < R_B$, is the typical outage with no secrecy and thus no secrecy outage. Accordingly, this data outage is not part of the secrecy outage and is out of our scope. Secrecy outage event occurs when Eve's channel capacity is higher than the difference $R_B - R_s$ conditioned on $C_B \geq R_B$, and the probability of such an event is the SOP.

A geometric relationship is lacking in the above definition of SOP in [11]. To characterize the secrecy outage event for the PPP distributed Eves, the ER, denoted by Θ, is defined by the geometric region only where Eves cause the secrecy outage event, i.e., $C_{Ei} > R_B - R_s, \exists z_{Ei} = (d, \theta) \in \Theta$. Accordingly, Θ can be represented by

$$\Theta = \{z : \ C(z) > R_B - R_s\}. \quad (7)$$

The i^{th} Eve will cause secrecy outage, if and only if $z_{Ei} \in \Theta$. At the same time, $C_B \geq R_B$ needs to be guaranteed.

Substituting (6) into (7) and rearranging d and θ, Θ can be transformed into

$$\Theta = \{z = (d, \theta) : \ d < D(\theta)\}, \quad (8)$$

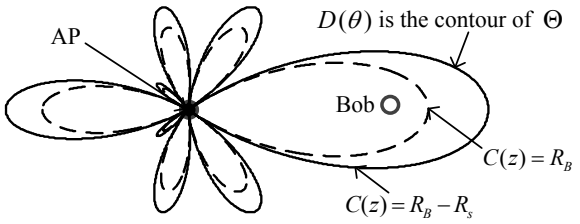

Fig. 2. Illustration of the ER Θ. $D(\theta)$ is the contour of Θ for given θ_B, which corresponds to $C(z) = R_B - R_s$; Bob should be within the curve $C(z) = R_B$ to guarantee a reliable transmission.

where

$$D(\theta) = [c_0 G^2(\theta, \theta_B)]^{\frac{1}{2}}, \tag{9}$$

where the constant $c_0 = \frac{P_t}{\sigma_n^2(2^{R_B - R_S} - 1)}$. $D(\theta)$ is a function only of θ for a given θ_B and the contour of Θ.

All locations within $D(\theta)$ have $C(z) > R_B - R_s$, giving a clear geometric meaning, as shown in Fig. 2. It can be shown from (9) that $D(\theta)$ (i.e., the shape of Θ) is mainly determined by $G(\theta, \theta_B)$.

Denoted by A, the quantity of Θ can be measured by the inner area of $D(\theta)$. Using (9), A in polar coordinates can be expressed by,

$$A = \frac{1}{2}\int_0^{2\pi} D^2(\theta)\,\mathrm{d}\theta = \frac{c_0}{2}\int_0^{2\pi} G^2(\theta, \theta_B)\,\mathrm{d}\theta. \tag{10}$$

A is measured in m^2 and depends on $G(\theta, \theta_B)$. Note that A is a general expression for any type of array.

A reliable transmission is guaranteed for Bob, if Bob is inside the dashed curve in Fig. 2, i.e., $C_B > R_B$. A secrecy outage event only occurs when $z_{Ei} \in \Theta$. Intuitively, given that Bob's reliable transmission is guaranteed, the smaller A is, the smaller number of Eves are statistically located in Θ, leading to less occurrence of the secrecy outage.

B. Spatial Secrecy Outage Probability

Any Eve at $z_{Ei} \in \Theta$ causes $C_{Ei} > R_B - R_s$ and this is referred to as a spatial secrecy outage (SSO) event with respect to the ER. The SSOP can be defined by the probability that any Eve is located inside Θ. To the best of our knowledge, the SSOP provides distinctive measure of the ER based security over the conventional SOP which does not have dynamic geometric implication; the SSOP emphasizes the secrecy outage caused by the spatially distributed Eves within a dynamic Θ.

We quantify the SSOP, denoted by p, to measure the secrecy performance. Particularly for given PPP-distributed Eves, the probability that m Eves are located inside Θ (with its area quantity A) is given by

$$\text{Prob}\{m \text{ Eves in } \Theta\} = \frac{(\lambda_e A)^m}{m!} e^{-\lambda_e A}. \tag{11}$$

Using (10) and (11), p can be quantitatively measured by referring to 'no secrecy outage' event that no Eves are located inside Θ and is given by

$$p = 1 - \text{Prob}\{0 \text{ Eve in } \Theta\} = 1 - e^{-\lambda_e A}, \tag{12}$$

where A is given by (10). It can be seen from (12) that for a given λ_e, p decreases along with A. The smaller p is, the less the spatial secrecy outage occurs. This results in the more secure transmission to Bob.

Remark 1: The probability p in (12) is positively correlated with the transmit power P_t via c_0. It is worth noticing that P_t influences the SSOP being independent of the array parameters. Therefore, when studying the impact of the array parameters, P_t is treated as constant within the constant c_0.

Note that the expression of p in (12) is a general expression for any type of array. Given the expression of $G(\theta, \theta_B)$ for arbitrary array, p can be numerically calculated. For the UCA, the closed-form expression of p can be derived in the following section to facilitate detailed theoretical analysis.

C. Derivation of Closed-form SSOP for UCA

In order to obtain the closed-form expression of p for a UCA, the closed-form expression of A should be obtained first, according to (12). To this end, θ should be first isolated to solve the integral in (10).

$$G^2(\theta, \theta_B) = \frac{1}{N}\sum_{i,j} e^{jkR[\cos(\theta_B - \psi_i) - \cos(\theta_B - \psi_j)]} \cdot e^{-jkR[\cos(\theta - \psi_i) - \cos(\theta - \psi_j)]}, \tag{13}$$

where $\sum_{i,j}$ represents $\sum_{i=1}^{N}\sum_{j=1}^{N}$ and $\cos(\theta - \psi_i) - \cos(\theta - \psi_j)$ can be further derived by

$$\begin{aligned}&\cos(\theta - \psi_i) - \cos(\theta - \psi_j)\\ =&2\sin(\theta - \frac{i+j-2}{N}\pi)\sin(\frac{i-j}{N}\pi).\end{aligned} \tag{14}$$

Let $W_{i,j} = 2\sin(\frac{i-j}{N}\pi)$ and $Z_{i,j} = \frac{i+j-2}{N}\pi$. Substituting (14) into (13), it can be derived that

$$G^2(\theta, \theta_B) = \frac{1}{N}\sum_{i,j} e^{jkRW_{i,j}\sin(\theta_B - Z_{i,j})} \cdot e^{-jkRW_{i,j}\sin(\theta - Z_{i,j})}. \tag{15}$$

According to $J_n(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{j(n\tau - x\sin\tau)}\mathrm{d}\tau$, substituting (15) into (10), A can be derived as

$$A = \frac{\pi c_0}{N}\sum_{i,j} J_0(kRW_{i,j}) e^{jkRW_{i,j}\sin(\theta_B - Z_{i,j})}, \tag{16}$$

where $J_0(\cdot)$ is the Bessel function of the first kind with order zero. The double summation of $J_0(\cdot)$ in (16) is intractable to analyze. Thus, A will be further simplified in the following. Let $A_{i,j}$ denote each summation term in (16), i.e.,

$$A_{i,j} = \frac{\pi c_0}{N} J_0(kRW_{i,j}) e^{jkRW_{i,j}\sin(\theta_B - Z_{i,j})}. \tag{17}$$

It can be deduced that $W_{i,j} = -W_{j,i}$ and $Z_{i,j} = Z_{j,i}$. Consider that $J_0(x)$ is an even function, it can be deduced that $A_{i,j} = A_{j,i}^*$. Furthermore, it is also noticed that $W_{i,j+N} = -W_{i,j}$ and $\sin(\theta_B - Z_{i,j+N}) = -\sin(\theta_B - Z_{i,j})$. Therefore, $A_{i,j} = A_{i,j+N}$. As a result, the summation of A in (16) can be formulated in a new way. To better illustrate the new summation, an extended table is created, as shown in Fig. 3, where $N = 4$. Instead of adding $A_{i,j}$ along the row and column, the summation is executed diagonally.

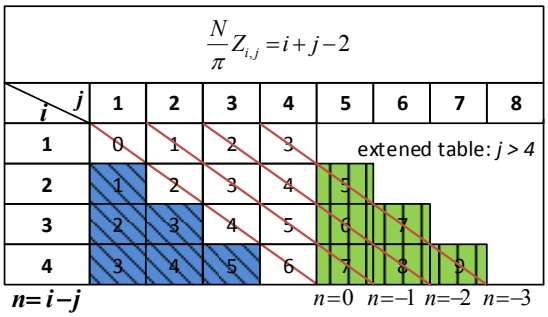

Fig. 3. Table for $Z_{i,j}$

For convenience, let $n = i - j$. Then, $W_n = W_{i,j} = 2\sin(\frac{n}{N}\pi)$. The terms $A_{i,j}$ on the red diagonal lines in the table have the same W_n. In the table, $\frac{N}{\pi}Z_{i,j}$ is allocated according to their indice i and j. Given $n = i - j$, it can be derived that

$$Z_{n,i} = Z_{i,j} = \frac{i+j-2}{N}\pi = \frac{2i-n-2}{N}\pi. \tag{18}$$

Thus, it can be derived that

$$A_{n,i} = A_{i,j} = \frac{\pi c_0}{N} J_0(kRW_n) e^{jkRW_n \sin(\theta_B - Z_{n,i})}. \tag{19}$$

Because $A_{i,j} = A_{i,j+N}$, the calculation of A can be executed by replacing the lower triangle in the original table (i.e., $i > j$) with the lower triangle in the extended table (i.e., $i > j - N$). In the new formation of A, which is a parallelogram table, the summation can be carried out along the diagonal lines from $n = 0$ to $n = -(N-1)$. For any n, there are N summation terms on the diagonal. Thus, (16) can be transformed into

$$A = \frac{\pi c_0}{N} \sum_{n=0}^{-(N-1)} \sum_{i=1}^{N} J_0(kRW_n) e^{jkRW_n \sin(\theta_B - Z_{n,i})} \tag{20}$$

In (20), the exponential can be expanded according to Jacobi-Anger expansion, i.e.,

$$e^{j\alpha \sin\gamma} = \sum_{m=-\infty}^{\infty} J_m(\alpha) e^{jm\gamma}, \tag{21}$$

where $J_m(\cdot)$ is the Bessel function of the first kind with order m. Substituting (18) into (20) and applying (21), (20) can be further derived by

$$A = \frac{\pi c_0}{N} \sum_{n=0}^{-(N-1)} \sum_{m=-\infty}^{\infty} J_0(kRW_n) J_m(kRW_n) e^{jm\theta_B} e^{j\pi\frac{m}{N}(n+2)} \sum_{i=1}^{N} e^{-j2\pi\frac{m}{N}i}. \tag{22}$$

When $m \neq lN$,

$$\sum_{i=1}^{N} e^{-j2\pi\frac{m}{N}i} = e^{-j2\pi\frac{m}{N}} \frac{1 - e^{-j2\pi\frac{m}{N}N}}{1 - e^{-j2\pi\frac{m}{N}}} = 0. \tag{23}$$

When $m = lN$, $l \in \mathbb{Z}$, we have

$$\sum_{i=1}^{N} e^{-j2\pi\frac{m}{N}i} = \sum_{i=1}^{N} e^{-j2\pi li} = N, \tag{24}$$

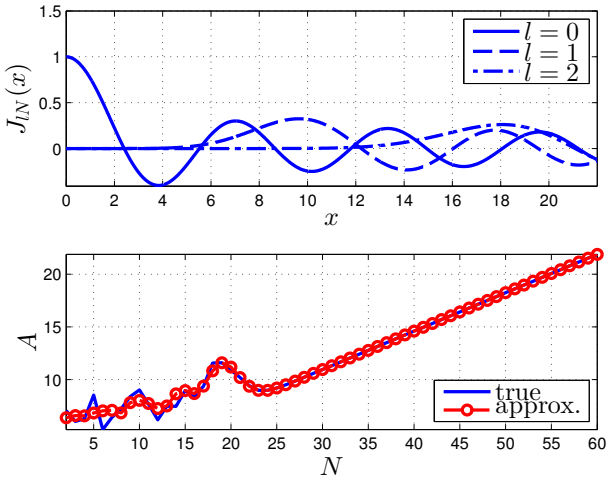

Fig. 4. Upper plot: $J_{lN}(x)$ for different l, $N = 8$; lower plot: true value and the approximation value of A versus N, $R = 1.75\lambda$, $\theta_B = 0°$.

and

$$e^{j\pi\frac{m}{N}(n+2)} = e^{jln\pi} e^{j2\pi l} = e^{jln\pi} = (-1)^{ln}. \tag{25}$$

Substituting (23)-(25) into (22), it can be derived that

$$A = \pi c_0 \sum_{n=0}^{-(N-1)} \sum_{l=-\infty}^{\infty} (-1)^{ln} J_0(kRW_n) J_{lN}(kRW_n) e^{jlN\theta_B} \tag{26}$$

Applying $J_n(-x) = (-1)^n J_n(x)$ to (26), the following expression can be obtained.

$$A = \pi c_0 \sum_{n=0}^{N-1} \sum_{l=-\infty}^{\infty} (-1)^{ln+lN} J_0(kRW_n) J_{lN}(kRW_n) e^{jlN\theta_B}. \tag{27}$$

Substituting (27) into (12), the closed-form expression of p is then obtained. Compared to (16), the summation in (27) consists of a finite summation of $J_0(\cdot)$ and an infinite summation of $J_{lN}(\cdot)$, which can provide asymptotic analysis. Since p is positively correlated with A, the impact of the array parameters (N and R) on p can be analyzed via (27).

IV. Impact of Array Parameters on SSOP

A. Impact of Number of Elements

Examples of $J_{lN}(x)$ are shown by the upper plot in Fig. 4, where $N = 8$ and $x = KRW_n$, according to (27). According to the expression of W_n, the range of x is fixed, i.e., $(0, 2kR]$, which is independent of N. For $R = 1.75\lambda$, $2kR = 7\pi$. When $l = 0$, $J_0(x)$ starts with the maximum value, i.e., 1, and has a damping envelope. When $l > 0$, $J_{8l}(x)$ starts from zero and only become comparable to $J_0(x)$ for a sufficiently large value $x_0(lN)$ that depends on $l > 0$ and N. For example, in the upper plot in Fig. 4, $J_8(x)$ is negligible in the range $x \in [0, 5]$ and $J_{16}(x)$ is negligible in the range $x \in [0, 12]$. In the $x \in (0, 7\pi]$, $J_{8l}(x)$ with $l > 2$ is negligible. In general, the infinite summation of $J_{lN}(x)$ in (27) can be approximated by a finite summation.

It can also be observed from the upper plot in Fig. 4 that the threshold $x_0(lN)$ that marks the upper limit of a range where $J_{lN}(x)$ is negligible increases along with the order lN. For $N = 8$ and $R = 1.75\lambda$, only $l = 0$, $l = 1$ and $l = 2$ contribute to A in (27). As N increases, $x_0(lN)$ also increases. When $x_0(N)$ becomes larger than $2kR$, $J_{lN}(x) \approx 0$, for $l > 0$, in the range $x \in (0, 2kR]$. In this case, A in (27) is approximated by

$$A \approx \pi c_0 \sum_{n=0}^{N-1} J_0^2(kRW_n). \tag{28}$$

For fixed R, the asymptotic behavior of A with N can be analyzed through (28). As N increases, $W_n = 2\sin(\frac{n}{N}\pi)$ takes more samples of $\sin x$ in the range of $x \in (0, \pi]$, thus $J_0^2(kRW_n)$ takes more samples of $J_0^2(x)$ in the range $x \in (0, 2kR]$. Because $J_0^2(x)$ is non-negative, the more samples are taken, the larger the summation of A is. However, when N is not very large, (28) is not valid and there does not exist a simple monotonic relationship between A and N.

The lower plot in Fig. 4 depicts the true value and the approximation of A versus N for $R = 1.75\lambda$. In the lower region of N, besides $J_0(kRW_n)$, $J_{lN}(kRW_n)$, $l > 0$, still contributes to the summation of A, leading to the fluctuating behavior. After $N \geq 19$, the summation of $J_{lN}(kRW_n)$, $l > 0$, becomes less significant and the approximation in (28) is very close to the true value. After $N > 25$, the asymptotic behavior of A is almost linearly increasing with N. Due to the positive correlation between p and A, p increases linearly with N when N is very large and fluctuates in the low region of N.

B. Impact of Radius

The impact of R can be analyzed from (27) without any approximation. For $n = 1, ..., N-1$ and $l \geq 0$, the envelopes of $J_{lN}(kRW_n)$ decreases and approaches 0 as R increases. Thus, the summation of A also decreases and approaches a certain value as R increases. Due to the difference in the converging speed of $J_{lN}(kRW_n)$, there will be some fluctuations.

Examples of $J_0(kRW_n)$ versus R for different n are depicted in the upper plot in Fig. 5. Except for $n = 0$ when $W_0 = 0$ and $J_0(0) = 1$, $J_0(kRW_n)$ graduately decreases as R increases. In the lower plot in Fig. 5, A versus R is shown for $N = 8$. It can be seen that A, i.e., p, decreases in general with fluctuations. However, in the low region of R, e.g., $R < 2\lambda$, the decreasing behavior is not very obvious.

V. Conclusions

This paper presented the closed-form expression of the SSOP for a UCA to analyze the security level of the ER-based beamforming. To this end, the concept of the ER and the SSOP were introduced for the free-space channel. Then, the double-summation of the Bessel functions of the first kind was obtained and simplified into the closed-form expression that is subject to asymptotic analysis. As the number of elements in a UCA grows larger, there is a linear relationship between the SSOP and the number of elements, whereas in the low region of the number of elements, the SSOP fluctuates. As the radius of a UCA increases, the SSOP gradually decreases with some fluctuations. For future work, the concept of the ER and the SSOP as well as the analysis of the array parameters can be extended to a Rician channel.

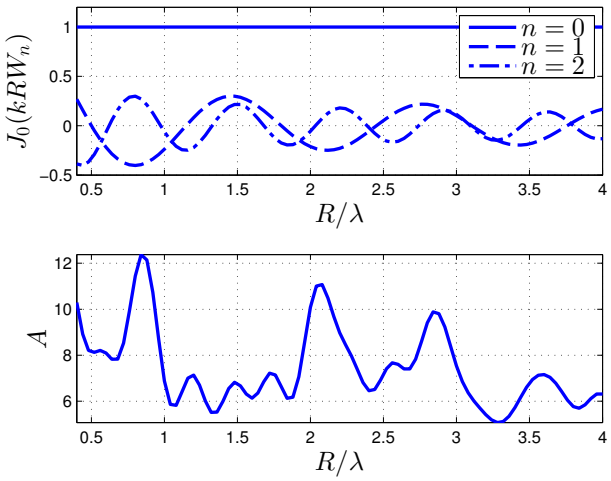

Fig. 5. Upper plot: $J_0(kRW_n)$ versus R for different n, $N = 8$; lower plot: A versus R, $N = 8$, $\theta_B = 0°$.

Acknowledgment

The authors gratefully acknowledge support from the Department of Education for Northern Ireland.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge: Cambridge University Press, 2011.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, pp. 1550–1573, Jan. 2014.

[4] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. on Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[5] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, 2014.

[6] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, 2016.

[7] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proc. IEEE 28th Int. Conf. on Distributed Computing Syst. (ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.

[8] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. IEEE 13th Canadian Workshop on Inform. Theory (CWIT)*, Toronto, Canada, Jun. 2013, pp. 214–218.

[9] J. Wang, J. Lee, F. Wang, and T. Q. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, 2015.

[10] B. Allen and M. Ghavami, *Adaptive Array Systems: Fundamentals and Applications*. New Jersey, USA: John Wiley & Sons, 2006.

[11] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, pp. 302–304, Mar. 2011.